(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/18729 A1

(51) International Patent Classification[7]: G06F 17/60

(21) International Application Number: PCT/US00/24756

(22) International Filing Date:
8 September 2000 (08.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/394,143 10 September 1999 (10.09.1999) US

(71) Applicant and
(72) Inventor: **TURGEON, Paul, Charles** [US/US]; 901 Sailors Reef, Fort collins, CO 80525 (US).

(74) Agent: **RICHARD, I., Samuel**; Goodwin, Procter & Hoar LLP, 7 Becker Farm Road, Roseland, NJ 07068 (US).

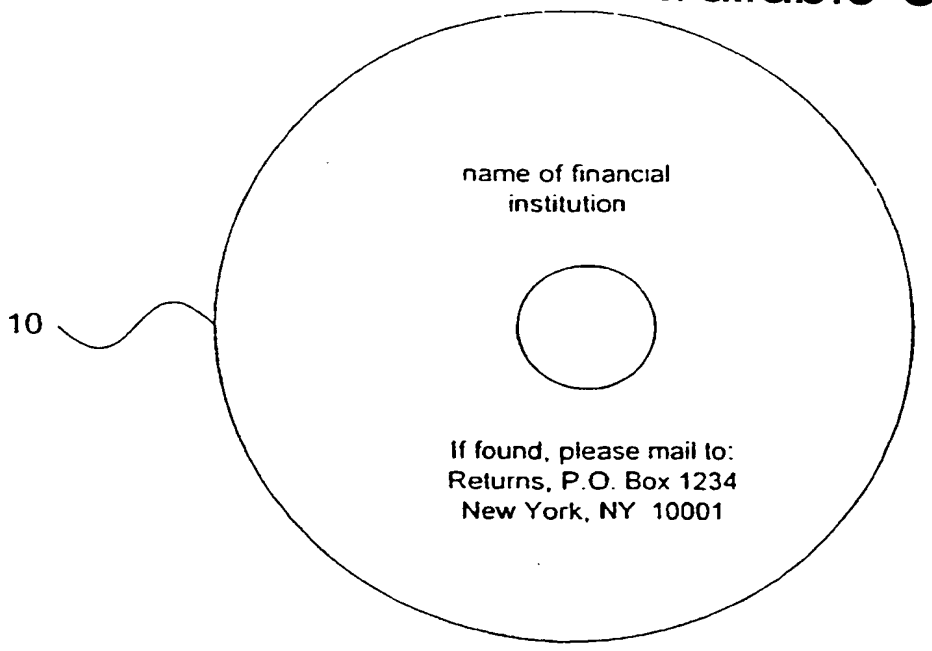
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR PROVIDING SECURE SERVICES OVER PUBLIC AND PRIVATE NETWORKS



(57) Abstract: A system and method for providing secure access over public communication lines using encrypted data on a removable, portable storage medium. In particular, the system and method pertain to the storing of encrypted customer data on a disk (10) in order to participate in trusted online commerce.

WO 01/18729 A1

SYSTEM AND METHOD FOR PROVIDING SECURE SERVICES OVER PUBLIC AND PRIVATE NETWORKS

COPYRIGHT NOTICE

BACKGROUND OF THE INVENTION

The present invention relates generally to electronic commerce and financial transactions. More particularly, the present invention relates to a system and method for providing secure environment to carry out electronic payments or other financial transactions over the Internet or other open network using the existing secure network, such as the automated teller machine (ATM) or point-of-sale (POS) network maintained by NYCE®, CIRRUS®, etc.

According to a recent article of a major business newspaper, electronic commerce via the Internet has seen a significant increase over the last year. As more and more people are attracted by the convenience and advantages of on-line shopping and to attract even greater number of customers, Web merchants need to address several issues concerning e-commerce.

First and foremost is the issue of security. Fraud in transactions may cost Web merchants many thousands of dollars in lost revenues. Furthermore, to do on-line purchases without any reservations, customers need to feel safe and assured that their confidential information will not be intercepted and misused by fraudulent users or by an unscrupulous merchant.

Also quite important is the second issue relating to on-line purchases, which is ease and convenience. Web merchants need Web sites that are user-friendly for e-commerce transactions, allowing even a novice computer user to purchase goods and/or services with minimum of

experience and knowledge. In addition, the amount of effort expended on transactions is likely to be directly proportional to the customer's attention span and time. Customers have to be enabled to do a transaction quickly on a Web site because of today's fast paced environment, or the Web merchant risks losing that customer.

Currently, to make a purchase over the Internet, Web merchants' sites require purchasers to complete a long form by providing personal information on-line. It is not uncommon for customers to fill in a form consisting of several pages. To enter all the requested information, the customers must scroll down to see the entire form or go to another page for continuation. In addition, if one of the requested items of information, such as name, address, e-mail address, phone numbers, etc., is accidentally skipped by the customer, he is required to return to the form to add the missing information. Furthermore, entering information on-line is subject to typographical errors causing problems for Web merchants and customers alike.

Furthermore, the conventional Web merchant site offers an option of phoning in the card information if the customer does not feel safe in providing his/her credit card or debit card information. Such option, however, partially defeats the advantages enjoyed by the merchant in selling goods and/or services via the Internet. Attending to customer information supplied over the phone is not only time-consuming but it requires the Web merchant to have staff for manning the phones and to maintain a sufficient number of lines. The additional expenses for the Web merchant and other attendant problems, such as forgetting to phone in the credit card information for example, present additional disadvantages of the current systems and techniques for performing electronic transactions over the Internet.

A need therefore exists for a system and method that addresses the above concerns and overcomes the disadvantages of conventional on-line payment systems.

BRIEF SUMMARY OF THE INVENTION

It is an object of the present invention to provide a secure environment for financial services conducted over a public network.

It is another object of the present invention to provide a method for purchasing goods or services on-line.

It is yet another object of the present invention to authenticate on-line users conducting financial services over a public network.

The above and other objects are achieved by a system for providing financial transactions over a public network accessible by customers via respective network access devices with modems and over a private network accessible by financial institutions via computers with modems. The financial institutions maintain respective financial accounts for the customers. The inventive system includes a network access device including a programmable controller for executing code and a memory for storing a browser software to interface with the public network. A customer uses the network access device and a computer-readable portable storage medium to access a customer's financial account via the public network. The computer-readable portable storage medium has encrypted and unencrypted information recorded thereon pertaining to the customer's financial account. A decryption processor, connected to the network access device via the public network, is operative to decrypt the encrypted information retrieved from the storage medium such that a financial institution, connected to the decryption processor via the private network, determines an access to the customer's financial account on the basis of the decrypted information.

In accordance with one aspect of the present invention, the unencrypted information selectively includes a name of the financial institution maintaining the customer's financial account, an audio message and advertising information pertaining to the financial institution.

In accordance with another aspect of the present invention, the computer-readable portable storage medium is a CD-ROM produced by a card production facility, based on a card

production file, for mailing the CD-ROM to the customer for use in the network access device.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated in the figures of the accompanying drawings which are meant to be exemplary and not limiting, in which like reference characters are intended to refer to like or corresponding parts, and in which:

Fig. 1a shows a block diagram of an e-commerce debit card as a computer-readable storage medium representatively exemplified by CD-ROM;

Fig. 1b shows another representation of the e-commerce debit card in block diagram form;

Fig. 2 shows a block diagram of the system for creating and issuing e-commerce debit cards for use in obtaining financial services over the Internet;

Fig. 3 shows a card issuance process flowchart for illustrating the operation of the system depicted in block diagram form in Fig. 2;

Fig. 4 shows, in block diagram form, a system which is utilized by a consumer to obtain financial services, for example to make secure debit purchases over a public network, such as the Internet, using his/her personal e-commerce card and personal computer; and

Figs. 5a, 5b, 5c and 5d show a transaction process flowchart for illustrating the operation of the system shown in Fig. 4.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As a general overview, the present invention includes a system and method for providing secure financial services over public communication lines, such as the Internet, intranet or any other network, using encrypted information on a removable, portable storage medium. In one embodiment of the present invention, information relating to a customer's bank account is stored to a disk which becomes his e-commerce debit card. For each customer, the stored information

may include customer's name, name and routing number of an issuing bank/financial institution, customer's account number, etc. This information is encrypted prior to being stored to the disk. Disks with the encrypted information are mailed to respective customers for use in debit purchases over the Internet.

In operation, when a customer desires to purchase goods and/or services on the Internet, he inserts his e-commerce debit card in the form of CD-ROM into a CD-ROM drive of a personal computer. The customer is then prompted to enter his Personal Identification Number (PIN) for the bank account used in the purchase transaction. A microprocessor in the personal computer executes instructions for retrieving the encrypted information from the CD-ROM and for transmitting the retrieved information to a server for a Web merchant's site for selling the requested goods and/or services. The server forwards the encrypted information, along with a request for debiting a specified amount, over the public communication lines to a secure network for automated teller machine (ATM) or point-of-sale (POS) transactions, such as NYCE® or Cirrus® networks. A processor located on the secure network processes the customer's debit request, and denies or approves the transaction based on the customer's available balance in his account. The results of such processing are returned to the Web merchant's site for completing or terminating the transaction.

According to this embodiment of the present invention, financial institutions issue e-commerce debit cards to those cardholders wishing to use their demand deposit accounts to make secure purchases over the Internet. A retail web site API specification is developed for use by vendors and builders of retail Web sites. In addition, a network decryption/interface module to which retail merchants connect their systems is also developed.

The card is loaded with a "blob" whose contents are encrypted using, for example, triple DES encryption. The blob contains the magnetic stripe information, typically found on conventional ATM cards, as well as the cardholder's name and statement address information.

The cardholders are given an "e-PIN" which will resolve the actual PIN. By using a separate e-PIN for the Internet commerce and similar transactions, the risk of introducing fraud at the ATM and POS is reduced.

The Web site API specifies how the "check out" screen (software) button works on Web merchant's sites and how the sites interface with the consumer computers and with merchants Web sites.

The network decryption/interface processor receives the encrypted blob from the merchant system, decrypts it and creates standard ISO 8583 debit POS messages, which it sends to the appropriate issuer processor. It also receives standard ISO 8583 debit POS response messages from the issuer processor and creates Web merchant response messages, which it sends to the retailer. These response messages contain only approval/denial response codes, trace information and, for consumer ease of use, may contain the information necessary to populate the shipping address screens on the Web merchant's site.

Card information is never available, except in highly secure encrypted form, throughout the life of the transaction at the consumer's PC or over the Internet. Only when a message reaches the network decryption/interface processor is the card information converted to a form normally used in network messages.

A representative transaction over a public network may be as follows:

- The consumer, using her/his PC, chooses the "Debit" button at the checkout stand on the retail Web merchant's site.
- The Web merchant's server downloads an active Web component module to a consumer's PC over a secure connection.
- The active Web module prompts the consumer to insert his/her debit card and enter e-PIN.
- The active Web module reads the blob from the card and sends the blob along with the e-PIN to the module on the Web merchant's site.

- The active Web module closes in the consumer's PC.
- The module on the Web merchant's site establishes a secure session (could be either a Web link or a dedicated link) with the network decryption/interface processor and forwards a request message containing the e-PIN, the blob and the merchant appended data.
- The network decryption/interface processor decrypts the blob, creates a POS request message, re-encrypts the PIN and sends an ISO 8583 debit POS purchase request to a network switch for forwarding to a financial institution for approval/denial code.
- The network decryption/interface processor, upon receipt of an approval response from the network switch, sends an approval response to the module on the Web merchant's site.
- The shipping information screen is then populated using the information in the response message for display to the consumer and for completion of the session.

Fig. 1a shows an e-commerce debit card as a computer-readable storage medium representatively exemplified by CD-ROM 10, containing customer information and other data for use in making debit purchases over the Internet in accordance with the present invention. The CD-ROM based card provides access to electronic commerce (e-commerce) from home personal computers using a CD-ROM drive (external or internal), without any modifications or additions to the hardware setup. The data stored on the e-commerce debit card is securely encrypted as described in detail below. Fig. 1b shows another representation of the e-commerce debit card which has the shape and size of the conventional debit card to provide familiar metaphor. The disk 12 depicted in Fig. 1b fits in a tray of a CD-ROM drive. It is understood, of course, that the removable computer-readable storage medium containing encrypted data according to the present invention may take on other shapes and sizes depending on customer preference and widespread usage of PC devices/drives. In another embodiment of the present invention, the removable computer-readable storage medium may include a programmable controller with memory for storing instruction code and data therein.

Fig. 2 shows a block diagram of the system for creating and issuing e-commerce debit cards for use in making debit purchases over the Internet. Shown in this figure is a block diagram of card issuance system 100 for generating a computer file of a predetermined format for storage on any computer-readable storage medium. The generated computer file contains information about the card holder's account and a financial institution which maintains his/her account. Representative information in the computer file may include account number, account holder's name, address, telephone number (day and/or evening). Further, the representative file information may include the name of the financial institution and may further include a routing number and address of the branch at which the account was opened. Card issuance system 100 also generates another file containing text, graphical banner advertisements, audio message, etc. relating to the issuing bank/financial institution.

Further shown in Fig. 2 is a block diagram of card production module 102 for generating yet another computer file based on data received from card issuance system 100 and from encryption module 104, as explained in detail hereinbelow. Card production module 102 may be implemented on a computer having a computer-readable storage medium for storing code and a programmable controller/microprocessor capable of executing the code for generating the computer file. The computer may be physically situated in card production facility 106 for providing cards to account holders in accordance with the present invention. As shown in Fig. 2, the computer is remotely located from card issuance system 100 such that secure dedicated lines communicatively couple card production facility 106 and card issuance system 100 for transfer of data and control signals.

Fig. 2 also shows a block diagram of encryption module 104 for encrypting data received from card production module 102. Encryption module 104 may be implemented on a physically secure computer having a computer-readable storage medium for storing code and a programmable controller/microprocessor capable of executing the code for encrypting data. The encryption computer may be physically situated in e-PIN mailer production facility 108 for

providing e-PIN mailers to account holders in accordance with the present invention. As representatively shown in Fig. 2, e-PIN mailer production facility 108 may be either remotely located from or co-located with card production module 102 and card production facility 106.

The operation of the system depicted in block diagram form in Fig. 2 is described next, with reference to the card issuance process flowchart shown in Fig. 3. In step 300 an information file containing account holder's information and bank information as described above is generated by card issuance system 100 for a particular customer. Another information file is further generated to include bank information screen and audio message for display on a PC monitor. In step 302 a PIN mailer file containing a personal identification number (PIN) for accessing the customer's bank account is generated by card issuance system 100. The customer's PIN is a predetermined number of alphanumeric characters individually generated for each account holder. The generated information files and PIN mailer file are then separately transferred from card issuance system 100 to card production module 102. In step 304, the PIN is extracted from the PIN mailer file, and is then sent from card production module 102 to encryption module 104 for encryption. In accordance with one embodiment of the present invention, the PIN is encrypted using first encoding data, such as public and private keys or other effective cryptographic algorithms as known to those skilled in the art, supplied by the financial institution that maintains the account. The encoding data, i.e., keys, are sent and stored separately from the information file that includes customer and bank information as described above.

Continuing with the description of Fig. 3, in step 306 encryption module 104 encrypts the customer's PIN and returns it to card production module 102. After receiving the encrypted PIN, card production module 102 sends the information file and the encrypted PIN to encryption module 104 for encrypting the entire information. That is, customer's PIN is encrypted separately and independently of the subsequent encryption of the entire information. According to one embodiment of the present invention, the entire information comprising account holder's

and bank's information as well as the encrypted PIN is encrypted using second encoding data, such as public and private keys or other cryptographic algorithms as known to those skilled in the art, supplied by the financial institution maintaining the account. Similar to the first encoding data, the second encoding data may be contained in the above-described information file.

In step 308 encryption module 104 encrypts the previously encrypted PIN and also encrypts account holder's and bank's information using the second encoding data, and returns the encrypted data to card production module 102. In step 310, after receiving the encrypted data, card production module 102 generates a card production file which is ready to be transferred to the customer's e-commerce debit card. The card production file includes the transaction routing information, unencrypted bank's logo and audio information, encrypted account holder's and bank's information, and twice encrypted customer's PIN as described above. In step 312, the card production file is transferred from card production module 102 to card production facility 106, wherein the file data is written to the customer's e-commerce debit card which is subsequently mailed to the customer who may or may not be the account holder.

In step 314 card production module 102 generates an e-PIN mailer file containing an e-PIN which resolves the customer's actual PIN. The e-PIN is a predetermined number of alphanumeric characters and is shorter in length than the actual PIN. The e-PIN is requested by an active Web module, such as an activeX module or Java applet, as explained in detail below. If correctly entered by a customer, the e-PIN in combination with the customer's PIN provides access to the customer's account for debit purchases. The generated e-PIN mailer file is then transferred from card production module 102 to e-PIN mailer production facility 108. In step 316 e-PIN mailer production facility creates the e-PIN mailer ready for delivery, and subsequently mails it to the bank's customer.

It will be appreciated that according to the present invention, no changes are required to the financial institution's card issuance and on-line authorization systems. In addition, there will

be no changes to the existing debit network on-line processing systems.

Fig. 4 shows, in block diagram form, a system which is utilized by a consumer to make secure debit purchases over a public network, such as the Internet, using his/her personal e-commerce card and personal computer in accordance with the present invention. Shown in Fig. 4 is a block diagram of personal computer (PC) 400 with Internet access and CD-ROM drive. The Internet access may be provided via a cable modem or a dial-up modem and browser software, such as Netscape® or Microsoft Explorer® in PC 400. In a preferred embodiment of the present invention, the disk drive is a CD-ROM drive for reading data from disks. Further shown in Fig. 4 is a block diagram of Web merchant's e-commerce site 402 which resides on Web host server 404 (computer). Also residing on Web host server 404 is merchant payment module 406 for use in the present invention as will be explained in detail below. PC 400 and Web host server 404 transfer data between each other via either publicly switched or dedicated lines of communication. Web host server 404 is communicatively coupled with decryption/interface processor 408 for processing customer's, bank's and Web site's data during the purchase transaction. Decryption/interface processor 408 is connected to network switch 410 for routing data to and from the financial institutions maintaining purchasing customers' accounts. Network switch 410 is part of the current secure network used by financial institutions to offer various services to consumers, such as cash withdrawal/deposit, bill payment, etc., via ATM and point-of-sale (POS) terminals. Decryption/interface processor 408 may be implemented on a remote, stand-alone computer connected via secure dedicated lines to network switch 410. Alternatively, decryption/interface processor 408 may locally reside with network switch 410. Located as nodes on the network are various financial institutions for holding customers' accounts. One representative financial institution is shown in block diagram form as block 412 connected to network switch 410 for transferring data therebetween via secure dedicated lines.

The operation of the system depicted in block diagram form in Fig. 4 is described next

with reference to a representative transaction over the Internet. The description below refers to the transaction process flowchart shown in Figs. 5a, 5b, 5c and 5d. As shown in Fig. 5a, in step 500 a cardholding consumer wishes to purchase goods and/or services over the Internet after logging on to the Web merchant's e-commerce site 402. In step 502, it is determined whether the consumer "clicked" on a screen button presented by the Web merchant's e-commerce site to indicate his desire to make a purchase with his e-commerce debit card. It is understood, of course, that in addition to the screen button, other forms of notification may be used by the consumer without departing from the spirit of the invention.

If the screen button was activated, then in step 504 Web host server (computer) downloads an active Web module, such as ActiveX or Java applet for example, to the browser running on the consumer's PC 400. Under control of the microprocessor in PC 400, in step 506 the active Web module is operative to prompt the consumer to place his e-commerce debit card in the CD-ROM drive. As an option, the active Web module may be additionally operative to open the CD-ROM drive. In step 508 it is determined whether the e-commerce debit card is in the CD-ROM drive. If so, in step 510 the microprocessor in PC 400 executing the active Web module code retrieves all data from the e-commerce debit card. The retrieved data includes, among other things, unencrypted text, graphics and audio data for display on a monitor. This personalized data, pertaining to the financial institution maintaining the consumer's financial account, includes a greeting to the customer and may optionally include an advertisement, in text, graphics and/or audio format, for other services available at the financial institution.

In step 512, under control of the microprocessor in PC 400 executing the active Web module code, the consumer is prompted to remove the e-commerce debit card from the CD-ROM drive. Optionally, the active Web module may be operative to open the CD-ROM drive while issuing the prompt to the consumer. In step 514 it is determined whether the e-commerce debit card was removed from the CD-ROM drive. If so, under control of the microprocessor in PC 400 executing the active Web module code, the CD-ROM drive is closed (if previously

opened), and the consumer is requested to enter his e-PIN for resolving the actual PIN as explained above, in step 516. If entered, as determined in step 518, the retrieved data including the e-PIN and encrypted cardholder's data are transferred via a Secure Socket Layer (SSL) connection from PC 400 to merchant payment module 406 at Web host server 404 (step 520). In step 521, after the data is uploaded to the Web host server 404, a memory in PC 400 (client station) is flushed to erase data used by the active Web module, which expires on PC 400. Upon receipt of the encrypted data, in step 522 a microprocessor in Web host server 404, by executing the code of merchant payment module 406, appends merchant specific transaction data to the received data. The appended transaction data identifies the merchant and/or Web merchant e-commerce site 402, and further includes data for indicating the purchase amount to be debited to the customer's account.

In step 524 the encrypted data and appended transaction data including the unencrypted e-PIN are transferred via a SSL connection from merchant payment module 406 to decryption/interface processor 408. In step 526 decryption/interface processor 408 decrypts the cardholder's data, and in step 528 it also decrypts and re-encrypts (translates) the PIN. Since the PIN cannot be "in the clear", the operation of decrypting and re-encrypting the PIN is known as PIN translation. In step 530 decryption/interface processor 408 adds the unencrypted e-PIN, supplied by the customer as explained above, to the re-encrypted PIN. This addition of two PINs is further combined with the decrypted cardholder's data by decryption/interface processor 408 to generate an ISO 8583 POS request message that contains, among other things, information necessary for routing the message to a financial institution. In step 532 the generated ISO 8583 POS request message is sent to network switch 410.

Further continuing with Fig. 5b, in step 534 network switch 410 forwards the received ISO 8583 POS request message to the appropriate financial institution. The message routing is performed on the basis of the bank routing number decrypted by decryption/interface processor 408. The transfer of information between network switch 410 and financial institution 412

occurs via the existing secure network, as mentioned above. In step 536 financial institution 412 receives the ISO 8583 POS request message and determines whether the supplied PIN is valid on the basis of the e-PIN and the encrypted PIN. If in step 538 it is determined that the access to the cardholder's account is legitimate, financial institution 412 debits the account for the requested purchase amount and generates an approval code message in step 540. If, however, the access to the consumer account is denied because of the incorrectly entered or fraudulent PIN or the account balance is insufficient for debiting the requested purchase amount, financial institution 412 generates a denial code message in step 542. In Fig. 5c, in step 544 financial institution 412 returns the appropriate code message (approval or denial) to network switch 410 for forwarding to decryption/interface processor 408 in step 546.

In step 548 decryption/interface processor 408 generates a response message on the basis of the code message received from network switch 410. If the received code message contains the transaction approval as determined in step 550, decryption/interface processor 408 inserts the cardholder's address data into the generated response message in step 552. The cardholder's address data was previously decrypted from the ISO 8583 POS request message as described above with reference to step 526.

The generated response message is then delivered to merchant payment module 406 via a SSL connection in step 554. If in step 556 it is determined that the response message contains address data, the Web merchant's e-commerce site populates the shipping fields with the cardholder's address data and displays this information, as well as the transaction amount, to the consumer for verification in step 558. Alternatively in another embodiment of the present invention, the shipping information may be formatted and supplied to the Web merchant's e-commerce site by a module external to Web host server 404. Upon reviewing the shipping address and transaction amount in step 560, the consumer determines whether the information is correct. If so, the consumer activates a "soft" button to accept the information in step 562. If information is incorrect or the consumer wishes to provide different shipping information, he can

change the address and other information in step 564.

If the response message does not contain address data as determined in step 556, the consumer is notified of the denied transaction via a message on the PC monitor in step 566. At this point and at the option of the Web merchant, the consumer may be given a brief explanation as to why the transaction was denied.

Continuing with the description of Fig. 5d, after finalizing the shipping and other information in step 562 or 564, the consumer is given the final chance to either accept or reject the transaction in step 568. If the consumer accepts, the transaction is completed by obligating the Web merchant to provide the requested goods and/or services according to the transaction in step 570. However, if the consumer changes his mind and declines to purchase the goods and/or services from the Web merchant, the transaction is reversed in step 572.

To reverse the transaction in this situation, payment module 406 in Web host server 404 prepares a message with the necessary customer information and sends the message to decryption/interface processor 408. Using the received information, decryption/interface processor 408 generates a financial reversal message in accordance with the ISO 8583 Interface Specification. The generated financial reversal message is sent to network switch 410 and subsequently to financial institution 412 for reversing the transaction. In the above example, financial institution 412 credits the previously debited amount to the customer's financial account in full compliance with the processing requirements as defined in the ISO 8583 Interface Specification.

The transaction reversal process may occur for other reasons. If, for example, the transaction "times out", a financial reversal message in accordance with the ISO 8583 Interface Specification is generated for processing by the financial institution. Namely, the transaction is aborted if a predetermined period of time allocated for response to a query or processing operation expires. This time-out, which may be intentional or unintentional due to hardware/software failure, may occur anywhere along the data transaction path, which is between

the consumer's network access device and the financial institution, inclusively. In this situation, the transaction reversal process is carried out in substantially the same way as described above.

While the present invention describes messages complying with the ISO 8583 Interface Specification for processing by the secure network such as NYCE®, it is understood that other secure networks may have different interface specification requirements. In this situation, decryption/interface processor 408 or any other processing device responsible for generating the network-compliant messages will generate an appropriate message in accordance with the necessary requirements by the secure network.

It will be appreciated that the present invention has no impact on the existing card issuance system or the existing authorization processing by the financial institution. Furthermore, the present invention does not require the completion of on-line forms as in the existing e-commerce techniques. In addition, the present invention offers a high level of protection against fraud, thereby reducing the merchant's processing expense.

According to the preferred embodiment of the present invention, the e-commerce debit card is issued to access the customer's checking/savings account at the bank. It will be appreciated, however, that the present invention is not limited to debit cards or debit accounts, such as checking and/or savings. Without departing from the spirit of the present invention, customer's credit card information, for example, may be stored to a computer-readable storage medium, and an e-commerce credit card may be produced by the system of the present invention and according to the process described hereinabove. Consequently, using the e-commerce credit card at a PC or other network access device, the customer may requests his credit-issuing financial institution to approve the on-line purchase by extending credit for the transaction amount. If approved, the customer completes the transaction at a Web merchant's site, as explained hereinabove in connection with the debit purchase.

In another embodiment of the present invention, by using public lines of communication the customer uses his e-commerce card to view information stored on a secure network. In

particular, a borrower may want to look at the status of his loan with a lending institution. By logging on to the lender's Web site and using the e-commerce card, the borrower may be entitled to view his loan account, the latest activity on the account, etc., in accordance with the above-described process and system of the present invention.

In this case, the borrower's e-commerce card is used to authenticate the cardholder, thereby enabling him to view personal and confidential information and also to avail himself of various services offered by the financial institution. For example, the borrower may set up on-line loan payments, whereby his checking account is regularly debited for the specified amount by accessing the lender's Web site and carrying out the steps of the transaction as described above with reference to Figs. 1-5d.

It will be appreciated by those skilled in the art that the present invention is not limited to PC 400 for carrying out the above-described functions. The customer may use a cellular telephone, a handheld digital assistant or any other network access device containing software for accessing a network, a programmable controller with a memory storage, and means for accommodating a removable computer-readable medium, whereby the data and/or program code in that medium is transferred to/from the programmable controller.

It will be further appreciated that while the above description with reference to the process flowcharts described in Figs. 3, 5a, 5b, 5c and 5d refers to modules, facilities and/or systems that generate, transfer, process, encrypt, send, receive, etc., it is understood that those and other operations are performed under the control of one or more processors/controllers executing computer readable program code. As known to those skilled in the art, a processor/controller retrieves the code, transfers the retrieved code to internal memory and executes code instructions from the internal memory to carry out those and other functions.

The program code, stored in computer readable media (including magnetic or optical media, and the like), directs a computer or other programmable device to function according to the flowcharts described above in connection with the preferred embodiment. An article of

manufacture is thus produced for carrying out the functions of the present invention.

While the invention has been described and illustrated in connection with preferred embodiments, many variations and modifications as will be evident to those skilled in this art may be made without departing from the spirit and scope of the invention, and the invention is thus not to be limited to the precise details of methodology or construction set forth above as such variations and modification are intended to be included within the scope of the invention.

WHAT IS CLAIMED IS:

1. A system for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, said system comprising:

a network access device including a programmable controller for executing code and a memory for storing a browser software to interface with said public network, a customer using said network access device and a computer-readable portable storage medium to access a customer's financial account via said public network, said computer-readable portable storage medium having encrypted and unencrypted information recorded thereon pertaining to said customer's financial account; and

a decryption processor, connected to said network access device via said public network, for decrypting said encrypted information retrieved from said storage medium such that a financial institution, connected to said decryption processor via said private network, determines an access to said customer's financial account on the basis of the decrypted information.

2. The system according to claim 1, further comprising a computer connected to said network access device via said public network, said computer hosting a site for goods or services available on-line, said computer comprising a microprocessor being operative to transfer an active module to said network access device in response to said customer requesting the access to said customer's financial account by using said computer-readable portable storage medium.

3. The system according to claim 2, wherein said active module contains code which is executed by said programmable controller in said network access device such that said unencrypted information is displayed to said customer who is requested to enter a first identifier related to

said customer's financial account.

4. The system according to claim 3, wherein said programmable controller is operative to transfer the entered first identifier and the encrypted information to said computer for forwarding to said decryption processor.

5. The system according to claim 4, wherein said decryption processor is operative to extract a second identifier pertaining to said customer's financial account from the decrypted information and to re-encrypt the extracted second identifier.

6. The system according to claim 5, further comprising a network switch located on said private network for routing the re-encrypted second identifier received from said decryption processor to said financial institution maintaining said customer's financial account for determining whether to approve the access to said customer's financial account.

7. The system according to claim 6, wherein said financial institution generates a code for indicating whether or not the access to said customer's financial account has been approved and transfers the generated code to said decryption processor via said network switch.

8. The system according to claim 7, wherein customer's address data is displayed to said customer on said network access device if said code represents an access approval.

9. The system according to claim 3, wherein the displayed unencrypted information includes a name of said financial institution maintaining said customer's financial account.

10. The system according to claim 3, wherein the displayed unencrypted information includes an

audio message pertaining to said financial institution maintaining said customer's financial account.

11. The system according to claim 3, wherein the displayed unencrypted information includes advertising information pertaining to said financial institution maintaining said customer's financial account.

12. The system according to claim 1, wherein said computer-readable portable storage medium is a CD-ROM.

13. The system according to claim 12, wherein said CD-ROM is produced by a card production facility, based on a card production file, for mailing said CD-ROM to said customer.

14. The system according to claim 13, wherein said card production file includes an encrypted first identifier pertaining to said customer's financial account and said unencrypted information pertaining to said financial institution.

15. The system according to claim 14, wherein said encrypted first identifier is generated by an encryption module for encrypting a first identifier.

16. The system according to claim 15, wherein said first identifier prior to the encryption is generated by a card issuance system which is further operative to generate a second identifier pertaining to said customer's financial account, the generated second identifier being transferred to a mailer production facility for mailing to said customer.

17. A method for providing financial services over a public network accessible by a plurality of

customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, said method comprising:

accessing a customer's financial account via said public network using a network access device and a computer-readable portable storage medium having encrypted and unencrypted information recorded thereon pertaining to said customer's financial account;

retrieving said encrypted and unencrypted information from said storage medium; and

decrypting the retrieved encrypted information such that a financial institution determines an access to said customer's financial account on the basis of the decrypted information.

18. The method according to claim 17, further comprising using said computer-readable portable storage medium in said network access device in response to an active module being downloaded to and executed at said network access device such that said unencrypted information is displayed to said customer.

19. The method according to claim 18, further comprising entering an identifier pertaining to said customer's financial account in response to the executed active module.

20. The method according to claim 19, wherein said unencrypted information includes a name of said financial institution maintaining said customer's financial account.

21. The method according to claim 19, wherein said unencrypted information includes an audio message pertaining to said financial institution maintaining said customer's financial account.

22. The method according to claim 19, wherein said unencrypted information includes

advertising information pertaining to said financial institution maintaining said customer's financial account.

23. The method according to claim 17, wherein said computer-readable portable storage medium is a CD-ROM.

24. The method according to claim 23, wherein said CD-ROM is produced on the basis of a card production file that includes an encrypted identifier pertaining to said customer's financial account and said unencrypted information pertaining to said financial institution.

25. The method according to claim 17, further comprising reviewing customer's address data displayed on a monitor of said network access device if said financial institution has approved the access to said customer's financial account.

26. A computer-readable portable storage medium having recorded thereon code, executable by a programmable controller, for providing financial services over a public network accessible by a plurality of customers via respective network access devices with modems and over a private network accessible by a plurality of financial institutions via computers with modems, said financial institutions maintaining respective financial accounts for said plurality of customers, said storage medium comprising:

first code means for storing encrypted information for accessing a customer's financial account via said public network; and

second code means for storing unencrypted information for displaying a name of a financial institution maintaining said customer's financial account in response to a customer using said storage medium in a network access device to request an access to said financial account.

27. The storage medium according to claim 26, wherein said unencrypted information further includes an audio message pertaining to said financial institution.

28. The storage medium according to claim 26, wherein said unencrypted information includes advertising information pertaining to said financial institution.

Fig. 1a

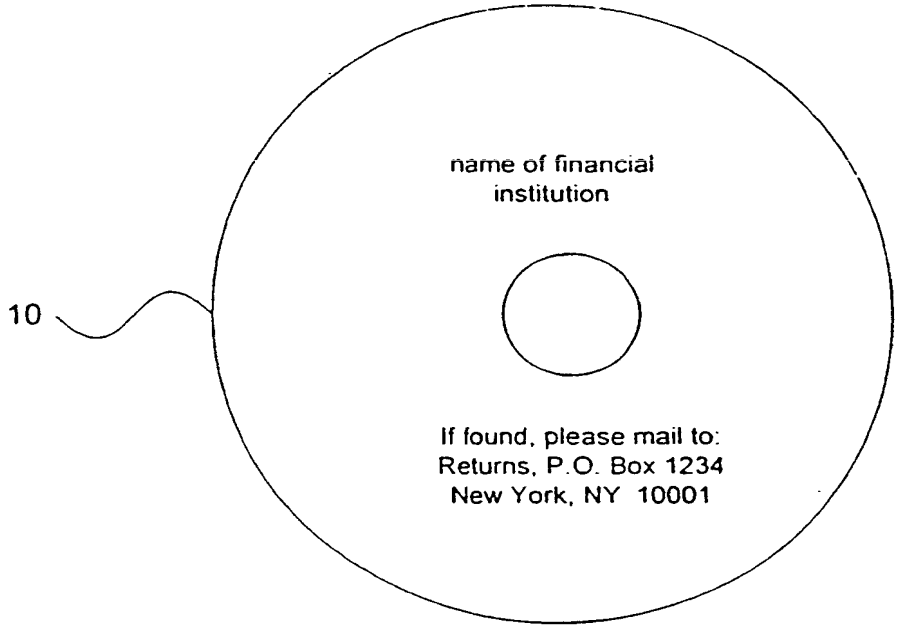
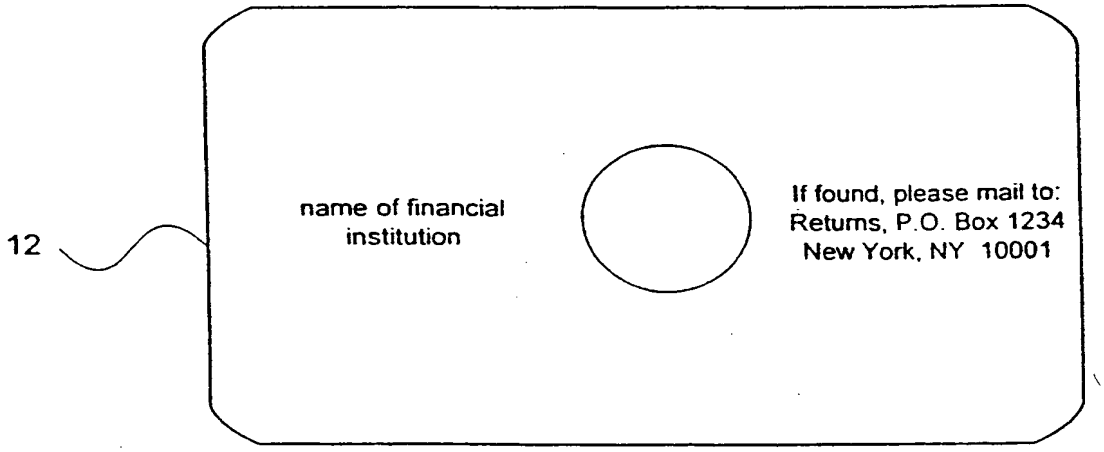


Fig. 1b



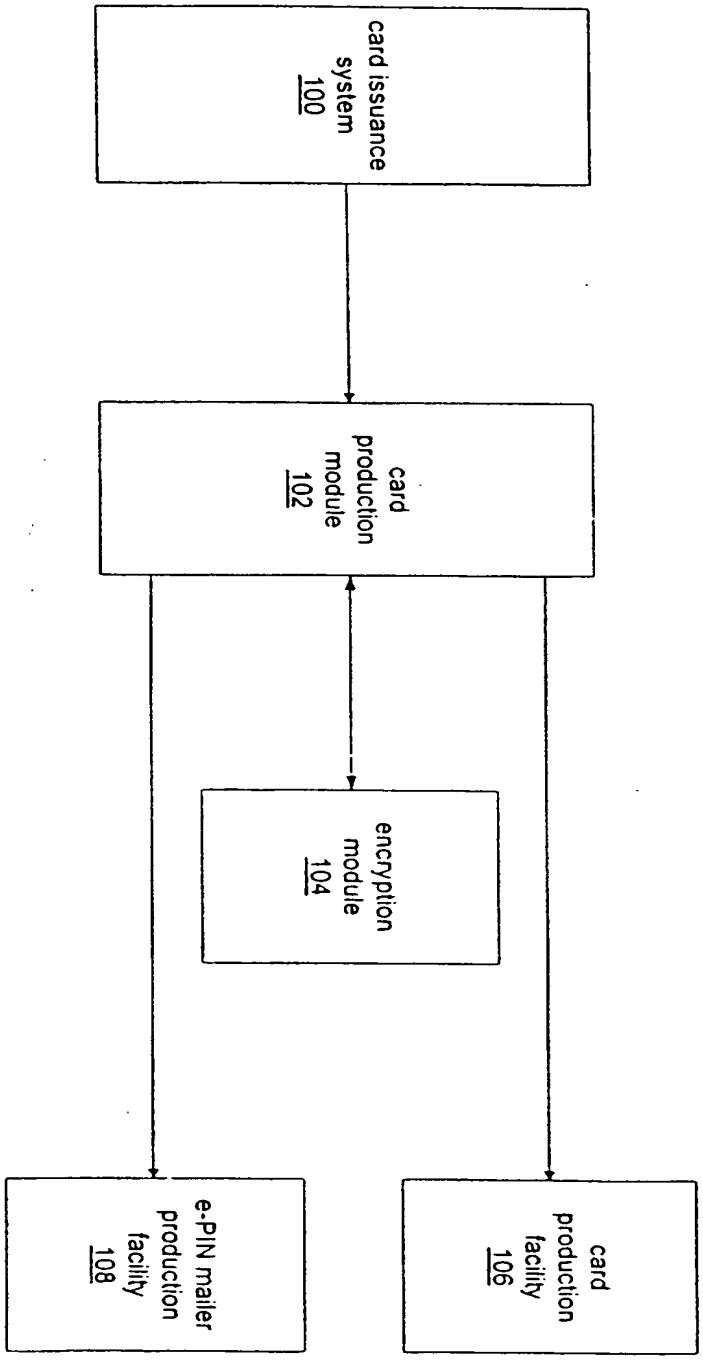
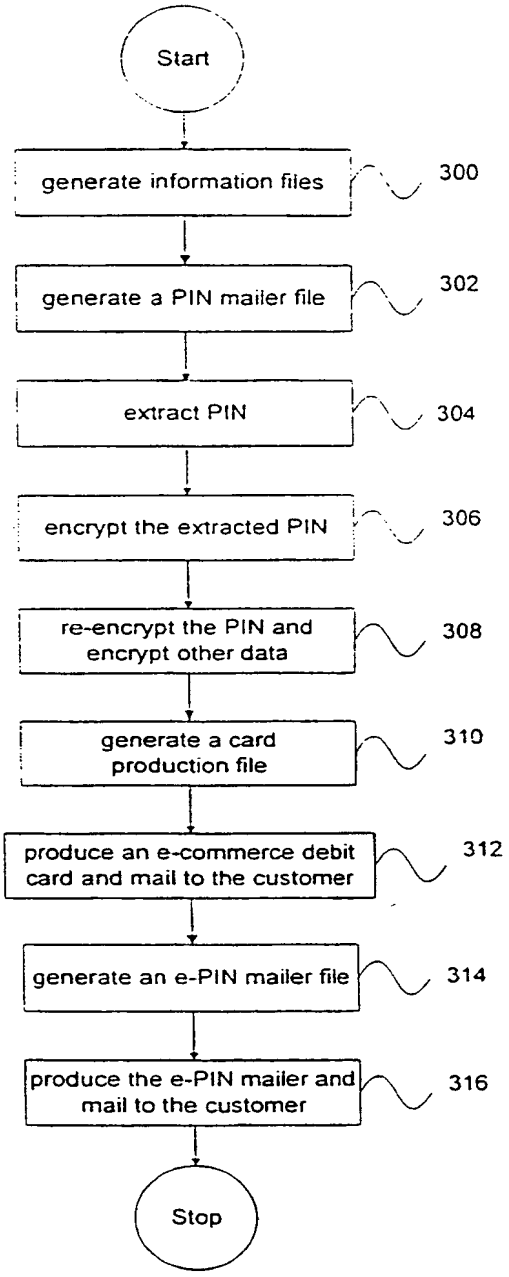


Fig. 2

Fig. 3



Sheet 3 of 8

Fig. 4

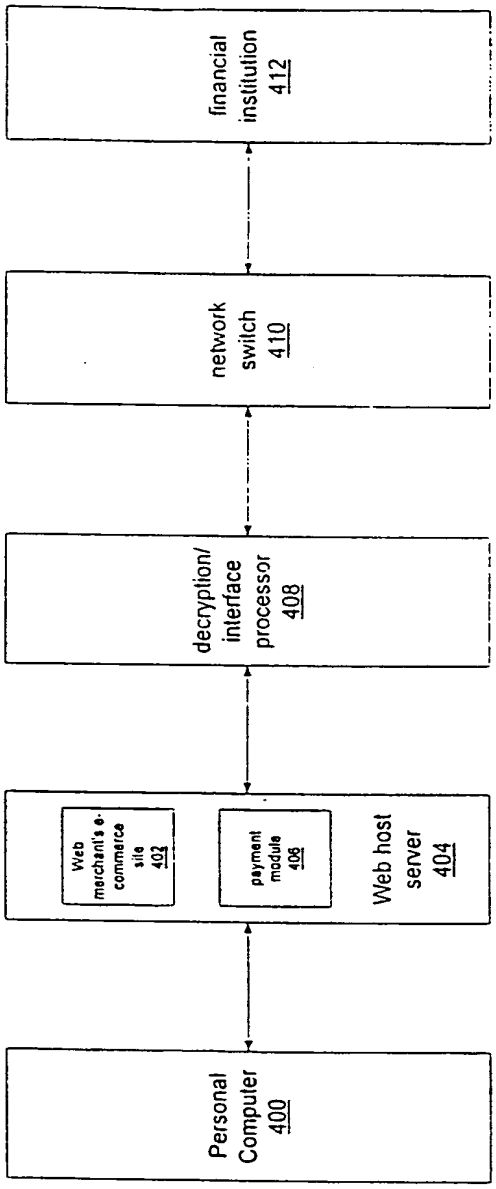


Fig. 5a

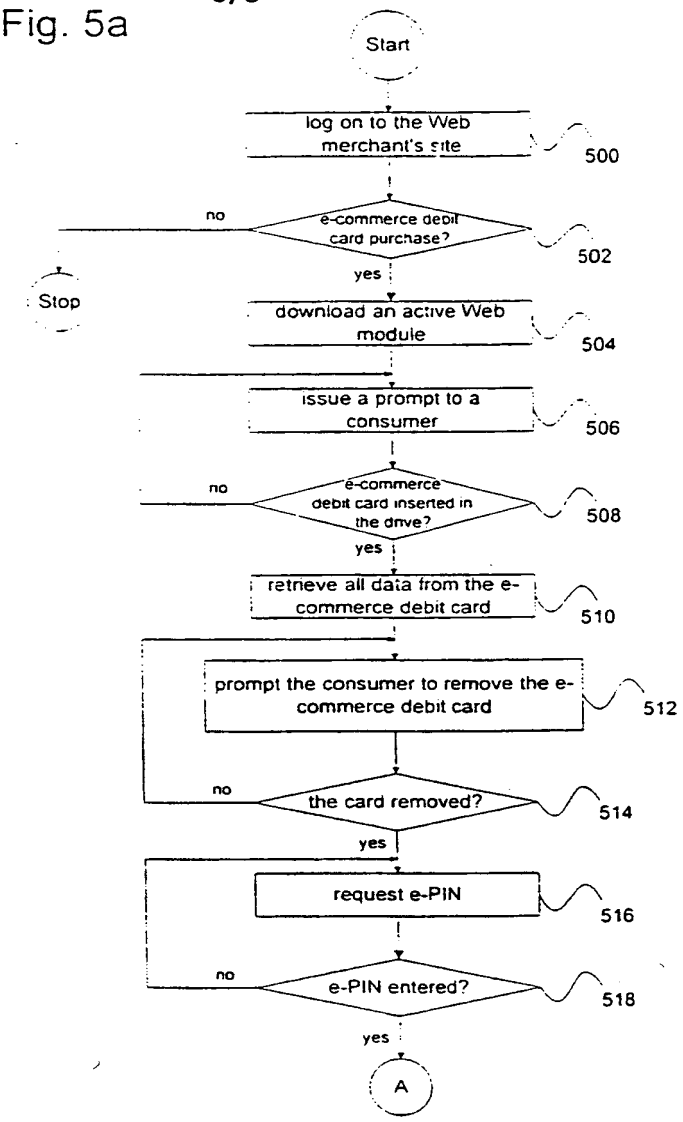


Fig. 5b

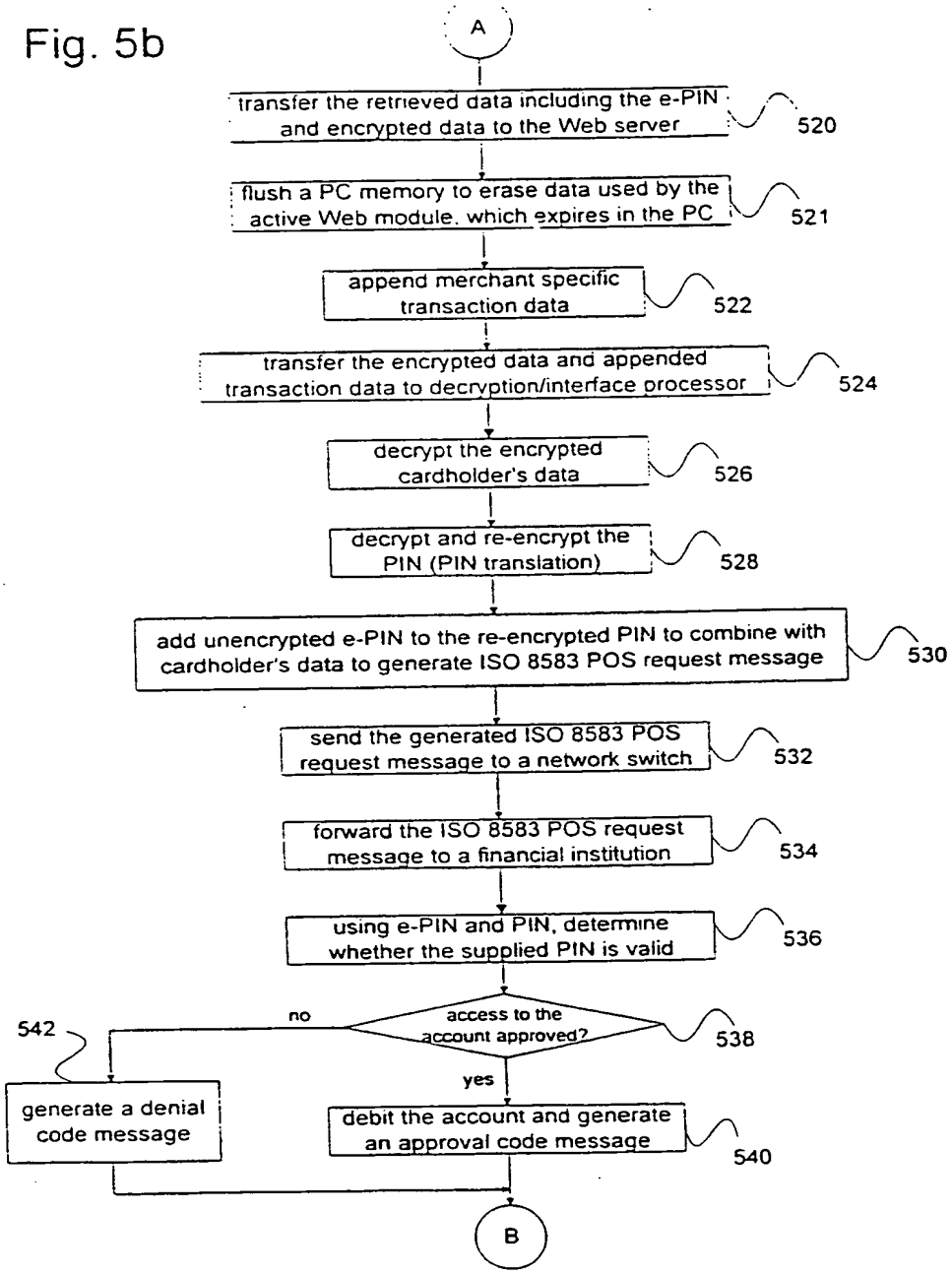


Fig. 5c

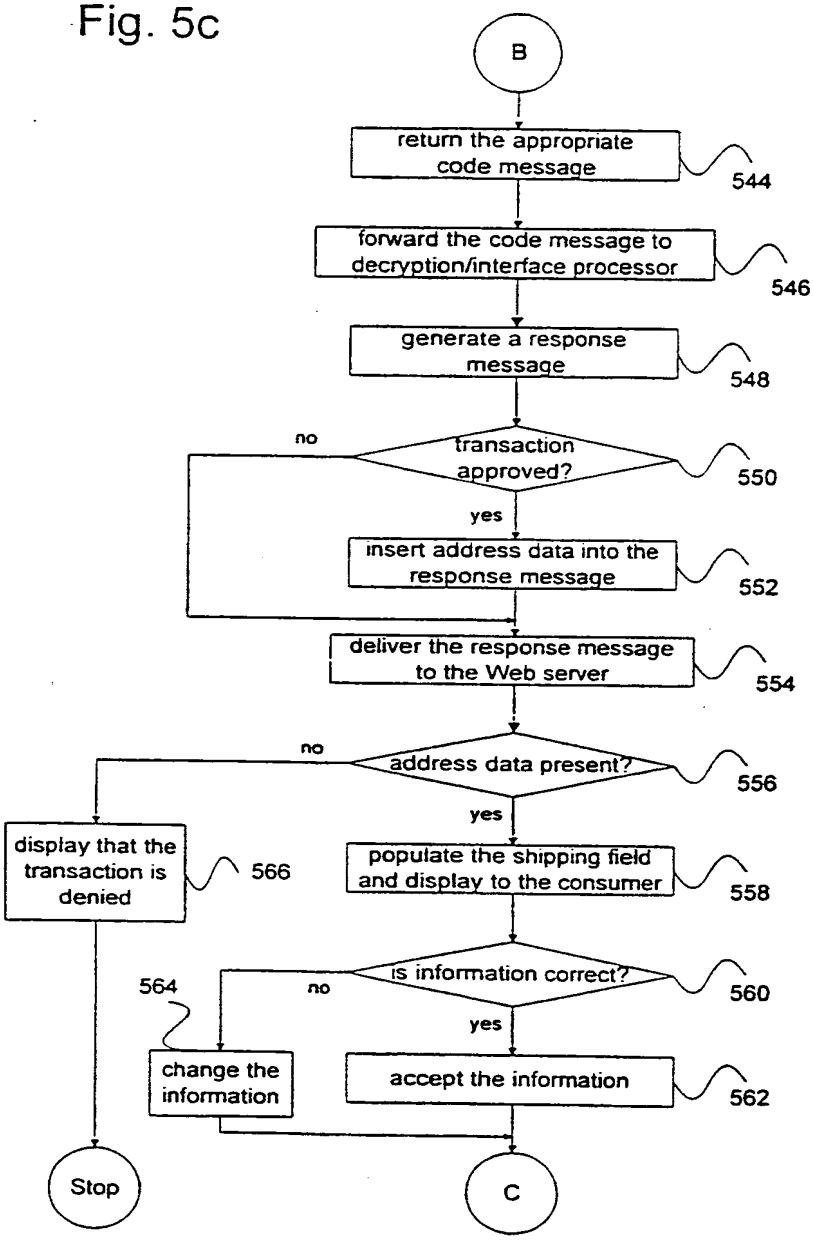
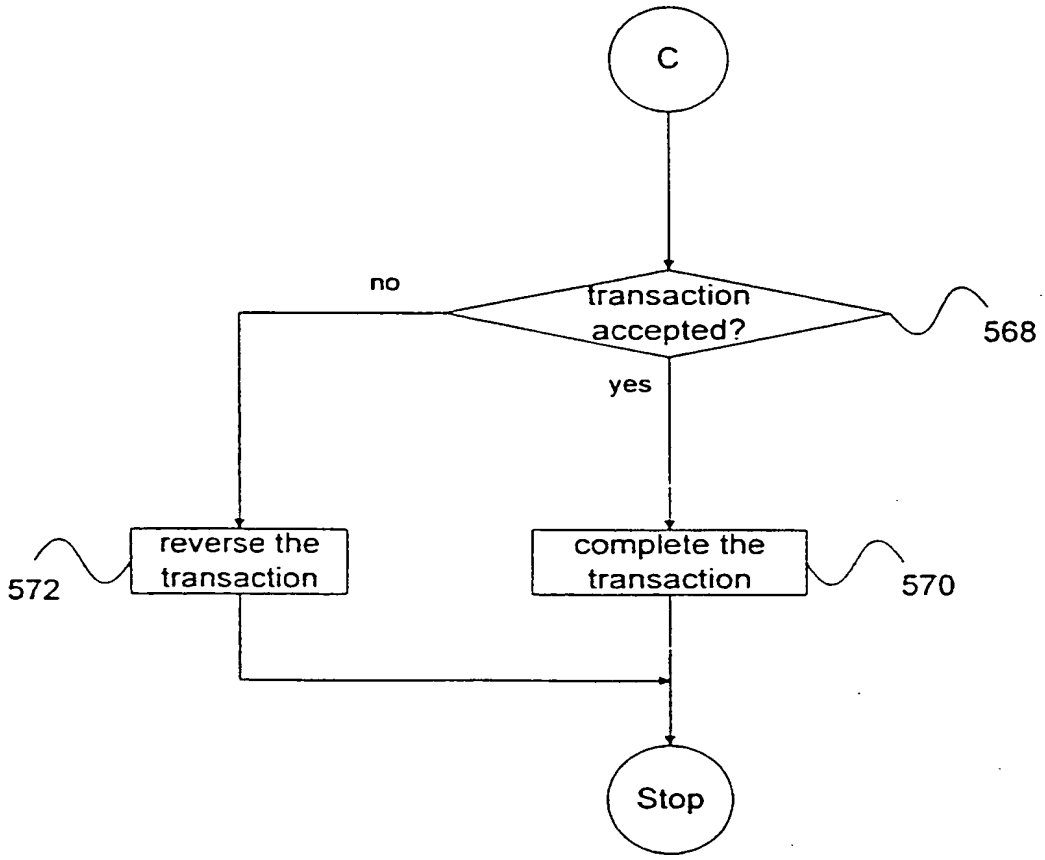


Fig. 5d



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/24756

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/60
US CL : 705/70

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/39, 705/42, 705/50, 705/53, 705/68, 705/69, 705/70

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST, search terms: encryption, online banking, cd-roms, optical disks, magnetic disks, remote banking, encoding

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,892,900 A (GINTER et al) 06 April 1999 (06.04.99) figures 1 and 1A, figure 5B, figure 35, figure 37, figures 41A, B and C; column 4, lines 14-28; column 7, lines 67; column 8, lines 20-28; column 9, lines 18-32; column 10, lines 31-46; column 12, lines 4-45; column 13, lines 50-67; column 18, lines 6-21; column 21,lines 60-67; column 22, lines 1-25; column 26,lines 37-67; column 27, lines 1-67; column 28, 1-16; column 30, lines 40-67; column 31, lines 64-67; column 32, lines 1-60; column 33, lines 65-67; column 35, lines 1-12; column 40, lines 62-67; column 41, lines 1-column 42, lines 35-59; column 49, lines 1-12; column 57, lines 45-65; column 58, lines1-50; column 62, lines 32-50; column 60, lines 58-67; column 61,lines 1-18; column 63, lines 13-27; column 67, lines 47-67; column 68, lines 1-27; column 309, lines 25-55	1-27
Y,P	US 6,073,160 A (GRANTHAM et al) 06 June 2000 (06.06.00) figures 8-10, column 4, 9-67; column 7, lines 24-36; column 9, lines 48-50; column 10, lines 13-64; column lines 6-27; column 19, lines 55-67; column 20, lines 1-67; column 23, lines 50-67; column 24, lines 47-67	1-27
Y,P	US 6,065,073 A (BOOTH) 16 May 2000 (16.05.00) figures 4A and B; column 1, lines 67; column 2, lines 1-67	1-4,6,12,13,17,23,24, 26

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 DECEMBER 2000	23 JAN 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer James P Trammell Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/24756

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 5,956,483 A (GRATE et al) 21 September 1999 (21.09.99) column 1, lines 15-45 and 58-67; column 2, lines 1-13	1-4,17,26

Form PCT/ISA/210 (continuation of second sheet) (July 1998)

European Patent Office

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 03 71 3916

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 01/18729 A (TURGEON, PAUL, CHARLES) 15 March 2001 (2001-03-15) * the whole document *	1-21	G07F19/00 G06F17/60
P,A	US 2002/038289 A1 (LAWLOR MATTHEW P ET AL) 28 March 2002 (2002-03-28) * abstract * * paragraph '0044! - paragraph '0045! * * paragraph '0078! - paragraph '0204! * * paragraph '0238! - paragraph '0353! *	1-21	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

G07F

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
The Hague	9 February 2005	Guenov, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C04)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 71 3916

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-02-2005

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0118729 A	15-03-2001	US 2003014371 A1	16-01-2003
		AU 7827900 A	10-04-2001
		CA 2422486 A1	15-03-2001
		WO 0118729 A1	15-03-2001
		US 2002152180 A1	17-10-2002
US 2002038289 A1	28-03-2002	US 6202054 B1	13-03-2001
		US 5870724 A	09-02-1999
		US 5220501 A	15-06-1993
		US 2004215564 A1	28-10-2004
		AT 182412 T	15-08-1999
		AU 7038791 A	18-07-1991
		CA 2069955 A1	09-06-1991
		DE 69033218 D1	26-08-1999
		DE 69033218 T2	13-04-2000
		EP 0504287 A1	23-09-1992
		WO 9109370 A1	27-06-1991